REMARKS

Patent claims 1, 3-5, 12-14, and 18-40 are pending in the present application. All of such claims have been finally rejected under 35 U.S.C. § 102(e) based upon U.S. Patent No. 6,725,260 issued to Philyaw.[1]

Method claim 1 is in independent form, and claims 3-5, 12-14, and 18-22 depend therefrom. Method claim 1 recites a method of preventing piracy of a given software application which includes the step of:

- requiring the user to communicate user data over a communications network to a remote service system, wherein the user data is partly derived from data that identifies the user, and partly derived from a unique identification code assigned to each authentic copy of the software application;

- archiving the user data in a data storage element of the remote service system;

- comparing received user data for each unique identification code with previously archived user data corresponding to the same unique identification code to determine whether a user is pirating the software application; and

- selectively transmitting service data to the user's computer from said remote service system when said remote service system determines that said service data should be transmitted.

The Examiner argues that these method steps are identically taught by Philyaw. In particular, the Examiner contends that the "comparing" step recited in claim 1 is disclosed in Philyaw's patent specification at col. 18, lines 37-42. The portion of the Philyaw specification relied upon by the Examiner is quoted below:

> "The message packet is then transmitted to interface 304 across the global communication network 306 to the ARS 308. The ARS 308 interrogates the message packet and performs a lookup function using the ARS database 310. If a match is found between particular

---

[1] Philyaw issued upon a patent application filed on May 10, 2000, just over one month before Applicant's application was filed. Applicant has not waived his right to establish, if necessary, that he made his invention prior to May 10, 2000.

parameters of the message packet, a return message packet is sent back to the PC 302 for processing."

The "message packet" referenced in the above-quoted passage is defined at col. 18, lines 12-16, as follows:

> "As part of the configuration for using the wand 1600, the PC 302 hosts wand software which is operable to interpret data transmitted from the wand 1600, and to create a message packet having the scanned product information and wand ID, routing information, and a user ID which identifies the user location of the wand 1600. The wand software loads at boot-up of the PC 302 and runs in the background. ... The wand program then inserts the necessary information into the browser program." (Emphasis added).

The system described by Philyaw within the above-quoted portions of the Philyaw patent specification is illustrated in Fig. 16 of the Philyaw patent. The user is provided with advertising information 1602 containing a machine-readable-code (MRC) 1606 that identifies a desired product, and which the user scans with an electronic wand 1600. Interface 1608 decodes MRC 1606 and adds an ID code for wand 1600. The user's computer, PC 302, includes scanning software that responds to the scanning signals provided by interface 1608, and as explained above, builds a communication packet including the product ID, the wand ID, and a user ID; this message packet is sent over the communications network 306 to the remote Advertiser Reference Server, ARS 308. Philyaw describes a database 310 associated with the remote ARS 308, which functions as follows:

> "Connected to the ARS 308 is a database 310 of product codes and associated manufacturer URLs. The database 310 undergoes a continual update process which is transparent to the user. As companies sign-on, i.e., subscribe to this technology, manufacturer and product information are added to the database 310 without interrupting operation of the source PC 302 with frequent updates. When the advertiser server address URL is obtained from the ARS database 310, it and the request for the particular advertiser product information is automatically routed back through the web browser on PC 302, over to the respective advertiser server for retrieval of the advertiser product information to the PC 302."

Philyaw also describes the manner in which ARS 308 "interrogates" the message packet; in this regard, Philyaw states:

> "Upon receipt of the message packet 400 from source PC 302, ARS 308 processes the information in accordance with instructions embedded in the overhead information. The ARS 308 specifically will extract the product code information from the received packet 400 and, once extracted, will then decode this product code information. Once decoded, this information is then compared with data contained within the ARS advertiser database 310 to determine if there is a "hit." If there is no "hit" indicating a match, then information is returned to the browser indicating such. If there is a "hit," a packet 402 is assembled which comprises the address of the source PC 302, and information instructing the source PC 302 as to how to access, directly in a "handoff" operation, another location on the network, that of an advertiser server 312."

Thus, when Philyaw describes a "lookup function using the ARS database 310" to determine if there is a match, Philyaw is not describing an examination of user data based in part on a unique identification code, and in part on user identification, as recited in Applicant's claim 1; rather, Philyaw is describing a comparison of a product information code contained in the message packet with product information contained in the ARS advertiser database 310. The ARS database 310 does not contain any user data.

Philyaw does describe the creation of "user profiles", and he even discloses an embodiment of his invention that includes a profile database 1308 (see Fig. 10). However, Philyaw is careful to distinguish his "user profile" database 1308 from the ARS database 310:

> "The profile database 1308 is a combination of the stored in profile database 1302 for all of the PCs 906 that are attachable to the system. This is to be distinguished from information stored in the database 310 of the ARS 308, the advertiser's database, which contains intermediate destination tables." (Emphasis added).

Thus, Philyaw fails to compare user data received by the remote computer with previously received user data for the same unique identification code. Philyaw also fails to disclose or suggest a method for preventing use of pirated software based upon such a comparison. Accordingly, Philyaw fails to teach or render obvious the method of preventing piracy of a software application as recited by claim 1 and the claims which depend therefrom.

Independent claim 23 recites a system for preventing piracy of a given software application including a user computer system on which a user desires to operate the software application, and a remote service computer system connected to the user computer system over a communications network. The user computer system transmits user data to the remote service computer system wherein the user data is partly derived from identifying data that identifies the user, and partly

derived from a unique identification code. The remote service computer system receives and stores the user data. Assuming that the remote service computer determines that the user is not pirating the software, then the remote service computer transmits service data to the user computer system required to activate at least part of the functionality of the software.

In rejecting claim 23, the Examiner contended that Philyaw discloses "a system for preventing piracy of a given software application". However, as noted above, Philyaw does not address the issue of preventing two different users from making use of the same copy of a given software application.

Claim 23 expressly states "said remote service computer system transmitting said service data to said user computer system over said communications network when it is determined that said user is not pirating said software application." Within the final Office Action, the Examiner cited two specific portions of the Philyaw patent specification as purportedly teaching such feature, namely, col. 18, lines 25-43, and col. 28, lines 25-60.

The first referenced portion, in col. 18, merely states that the wand software hosted by PC 302 creates a message packet having a scanned product ID, a wand ID, and a user ID which identifies the user location of the wand 1600. The wand program inserts necessary information into the browser program and transmits a message packet across the network 306 to ARS 308. ARS 308 interrogates the message packet and performs a lookup function using the ARS database 310. If a match is found, a return message packet is sent back to the PC 302 for processing. However, as explained above, the interrogation of the message packet is limited to extracting the product code and comparing it to a series of product codes saved in ARS database 310. There is no evaluation made of the identifying user data to determine whether the current user is attempting to pirate a copy of the software application already associated with a different user.

The second portion of the Philyaw patent specification relied upon by the Examiner, in col. 28, again relates to a lookup process, this time using "transaction code information". Philyaw defines a transaction code as a code associated with particular configuration information and embedded within document 1602 which is scannable or readable by wand 1600. Philyaw uses the transaction code to obtain the network address of the Vendor Web Site, VWS 2504 by performing a

lookup operation in Vendor Reference Server VRS 2500. The lookup operation uses the transaction code information as a parameter or a pointer to find the appropriate network server address in the database 2502 from which to access the relevant configuration information. Per decision block 2718, if there is a match between the transaction code and a value in database 2502, then flow is transferred to function block 2724 where a second message packet containing the matched network address, user profile information for identifying a user, and the transaction code is assembled and routed to the user PC 302, and then to the VWS 2504.

Once again, none of these steps serves to preclude a software pirate from making use of a software application using a copy of the software that is already being used by another user. Accordingly, the portions of the Philyaw disclosure relied upon by the Patent Examiner do not disclose or suggest a remote service computer system that transmits to the user computer system, over the communications network, service data that is required by a user to activate at least part of the functionality of the software application, after determining that the user is not pirating the software application.

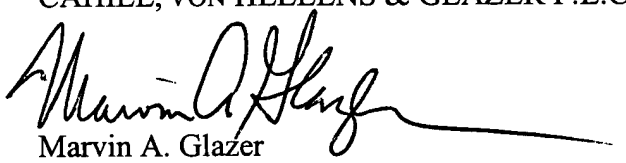
Independent claim 31 recites a method of preventing piracy of a given software application that requires the user to communicate user data over a communications network to a remote service system, wherein the user data is partly derived from data entered by the user into the user's computer system, and which identifies the user, and partly derived from a unique identification code associated with a particular authorized copy of the software application. Claim 31 further recites the step of examining the user data received by the remote service system to determine whether the user is pirating the software application; if not, then the further step of selectively transmitting service data to the user's computer from the remote service system is performed to activate at least part of the functionality of the software application . Independent claims 35 and 38 are each similar to claim 31, except that claims 35 and 38 do not expressly recite the step of requiring the user to enter into the user's computer the data that identifies the user (it may have

already been entered). However, all of such claims recite the step of "examining user data received by the remote service system ... to determine whether the user is pirating the software application". For the reasons noted above, Philyaw does not disclose or suggest this step.

For the foregoing reasons, independent claims 1, 23, 31, 35 and 38 recite subject matter that is neither anticipated by, nor suggested by, the cited patent to Philyaw. Accordingly, Applicant respectfully submits that the pending claims are patentably distinct from the art of record, and that the present application is in condition for allowance, which action is earnestly requested.

Respectfully submitted,

CAHILL, VON HELLENS & GLAZER P.L.C.



Marvin A. Glazer
Registration No. 28,801

155 Park One
2141 East Highland Avenue
Phoenix, Arizona 85016
Ph. (602) 956-7000
Fax (602) 495-9475
Docket No. 6589-A-2